

Security Building Blocks for e-Business

A yellow line graphic that starts at a dot on the right side of the title, extends horizontally to the left, then turns downward at a right angle, ending at another dot on the left side of the speaker's name.

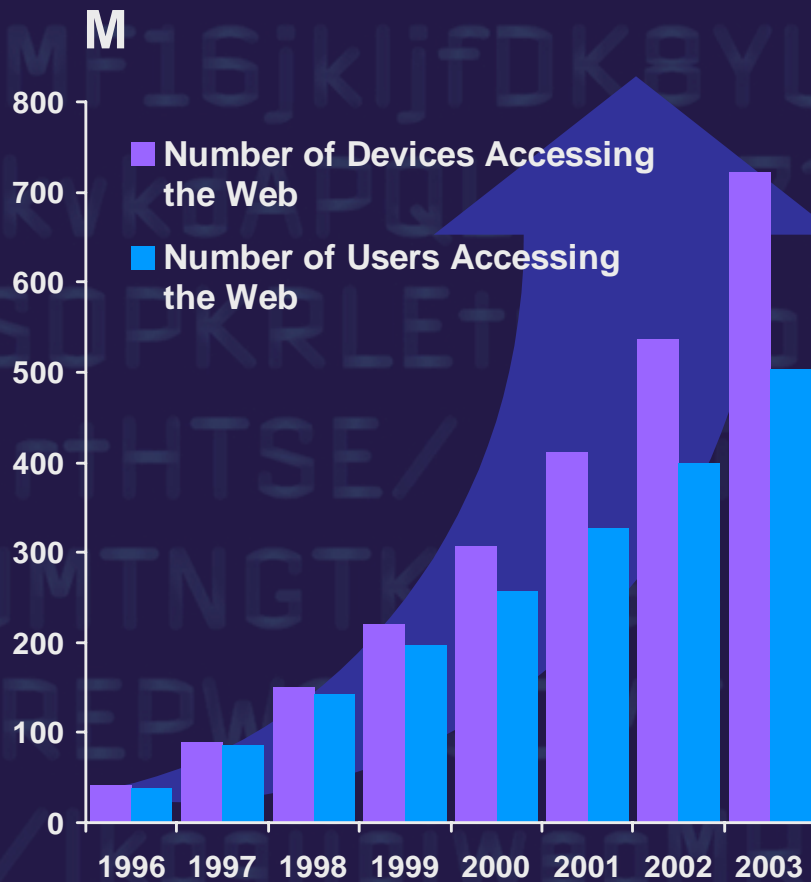
Gregory S. Lang
Vice President
Network Communications Group
Intel Corporation

January 19, 2000



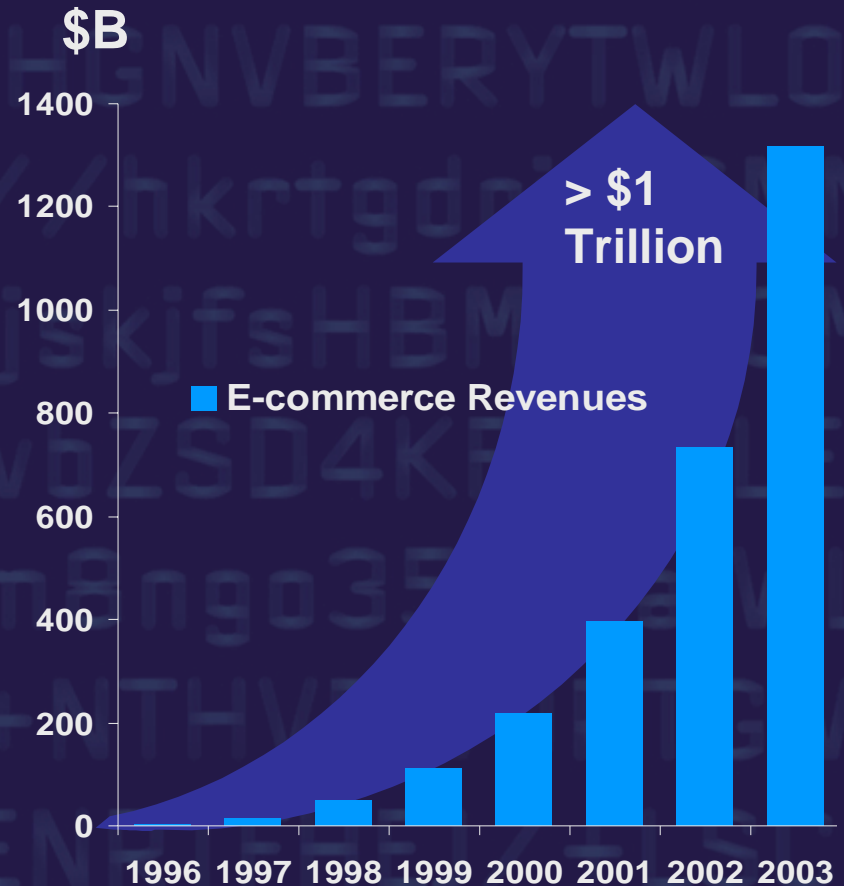
The Emerging Internet Economy

Worldwide



Source: IDC; The Global Market Forecast for Internet Usage, June 1999

Worldwide



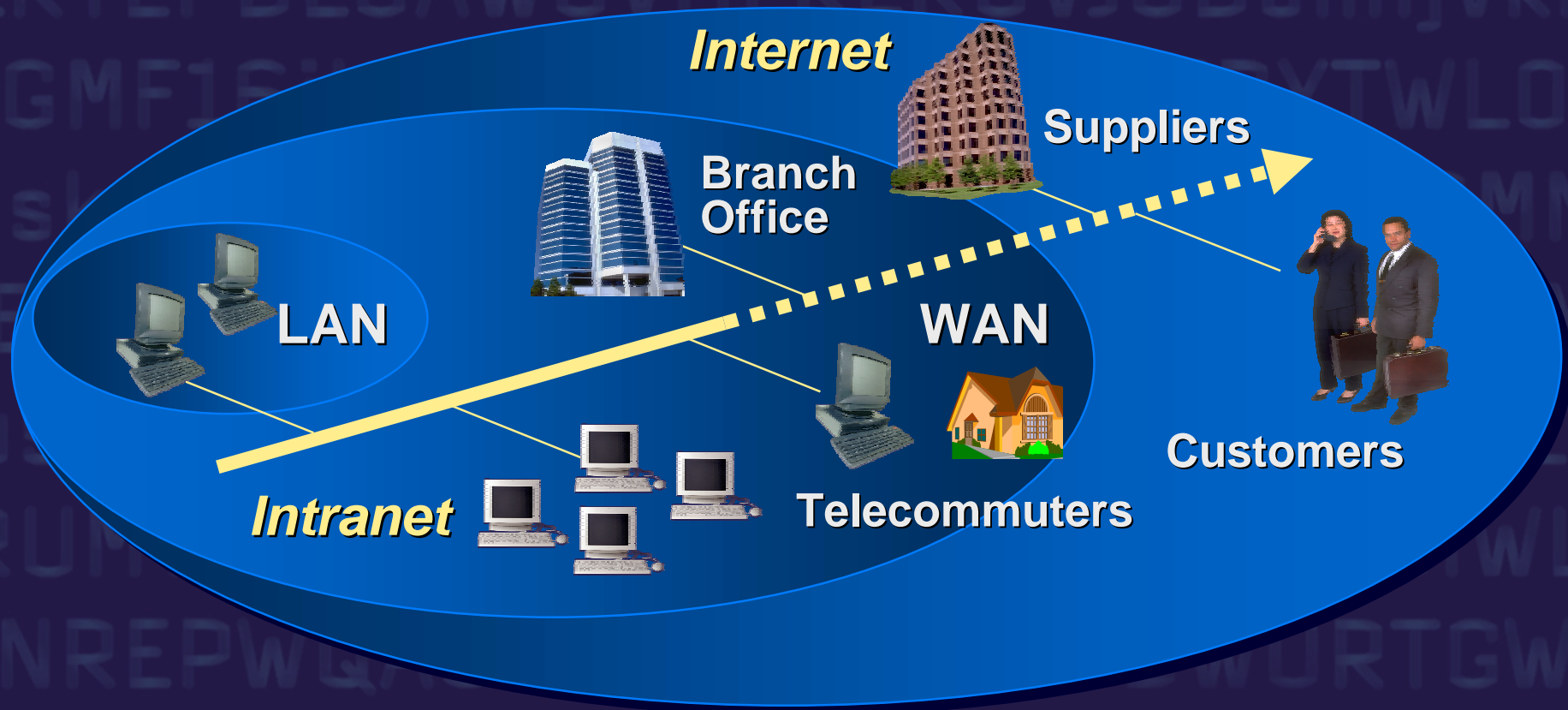
Source: IDC; The Global Market Forecast for Internet Usage, June 1999





*We Are Moving Towards a
World of a Billion Connected
People
and
a Trillion Connected Dollars*

The Internet is Changing Today's Business Model



**There is One Enterprise and it's Global.
There is One Network and it's the Internet.**

Evolution of the New Economy



Increased Value on the Internet



Threat Follows Value

The Internal Threat

Companies Detecting Unauthorized Use
in the Last 12 Months

Insider Abuse of
Net Access

97%

Unauthorized Access By
Insiders

55%

Denial of Service

32%

System Penetration
By Outsiders

31%

Theft of Proprietary Info

25%

Sabotage

13%

**Breaches From
Within The LAN**



Source: 1999 CSI/FBI Computer Crime & Security Survey

The Electric Car



1975

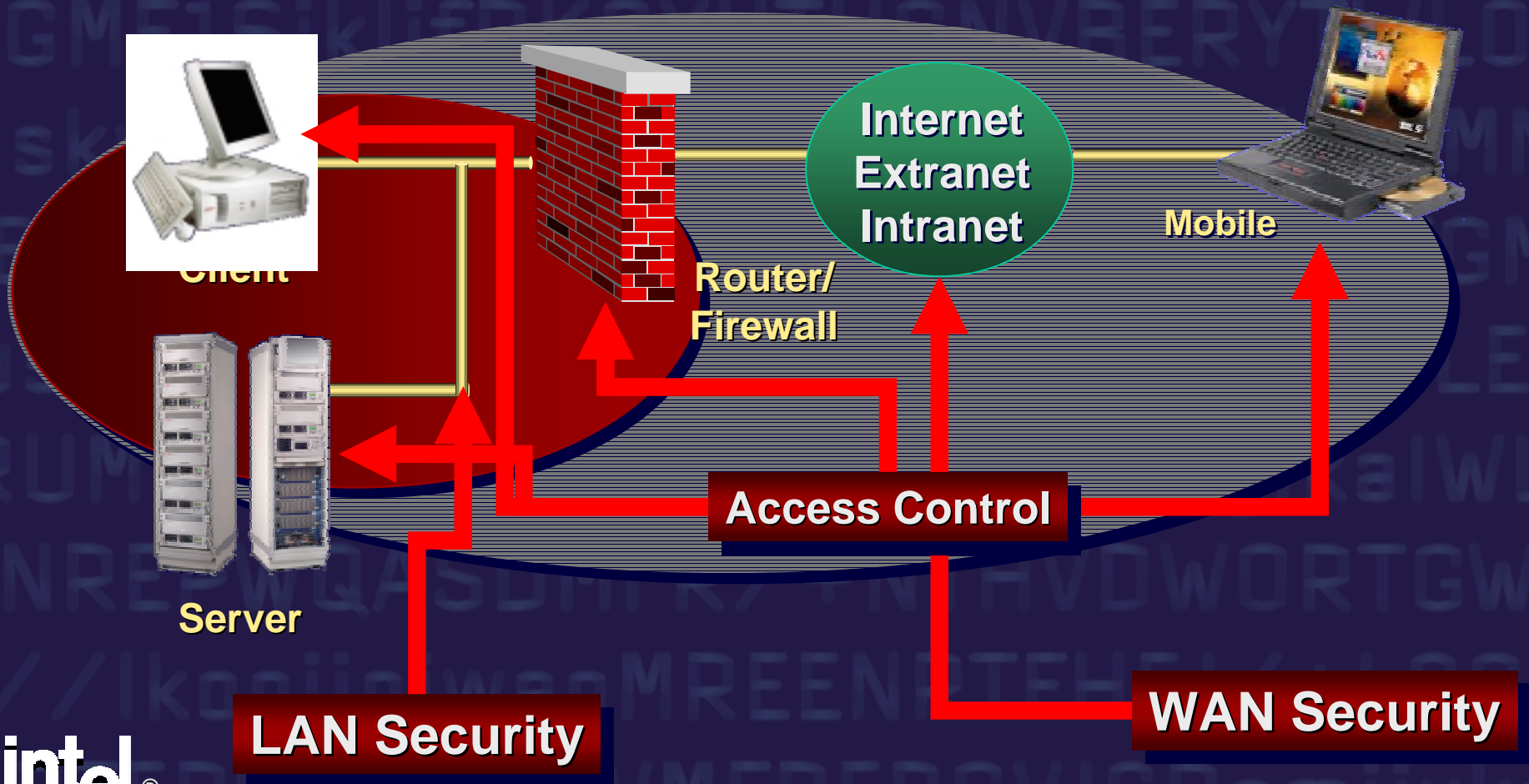
TODAY



Making it Mainstream

- **No-compromise performance**
- **Compatible infrastructure**
- **Affordable**
- **Easy to use**

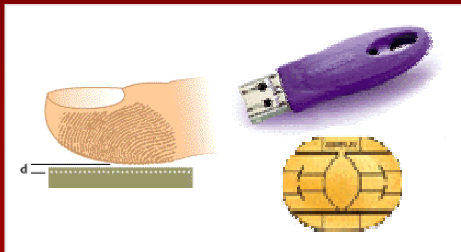
Elements of the Trusted Network



Elements of Trusted *Clients & Servers*

Authentication

*IPSec
Biometric
Smart Cards
/Tokens*



Firmware Controls

*Boot Integrity Services
Passwords
DriveLock*
QuickLock*/QuickBlank**



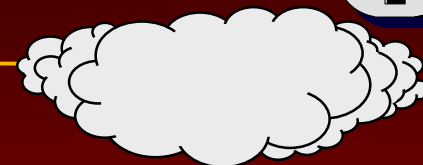
Physical Controls

*Hood and cable locks
Smart cover lock
Security screws*



Remote Management

Alert on LAN
Chassis intrusion
Missing processor
Presence Heartbeat*

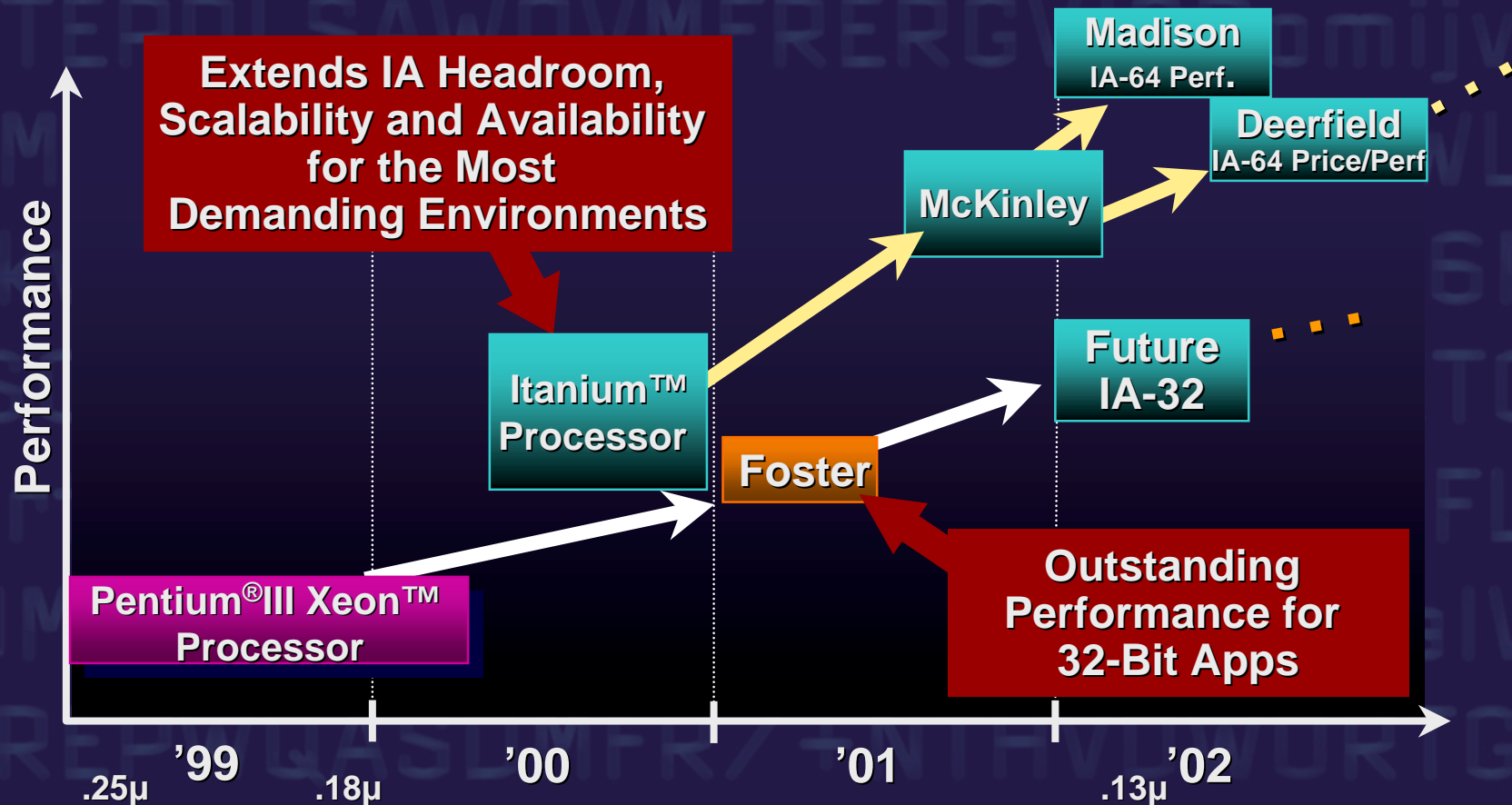


Server Performance



Building Block Enablers

Intel Servers & Workstations



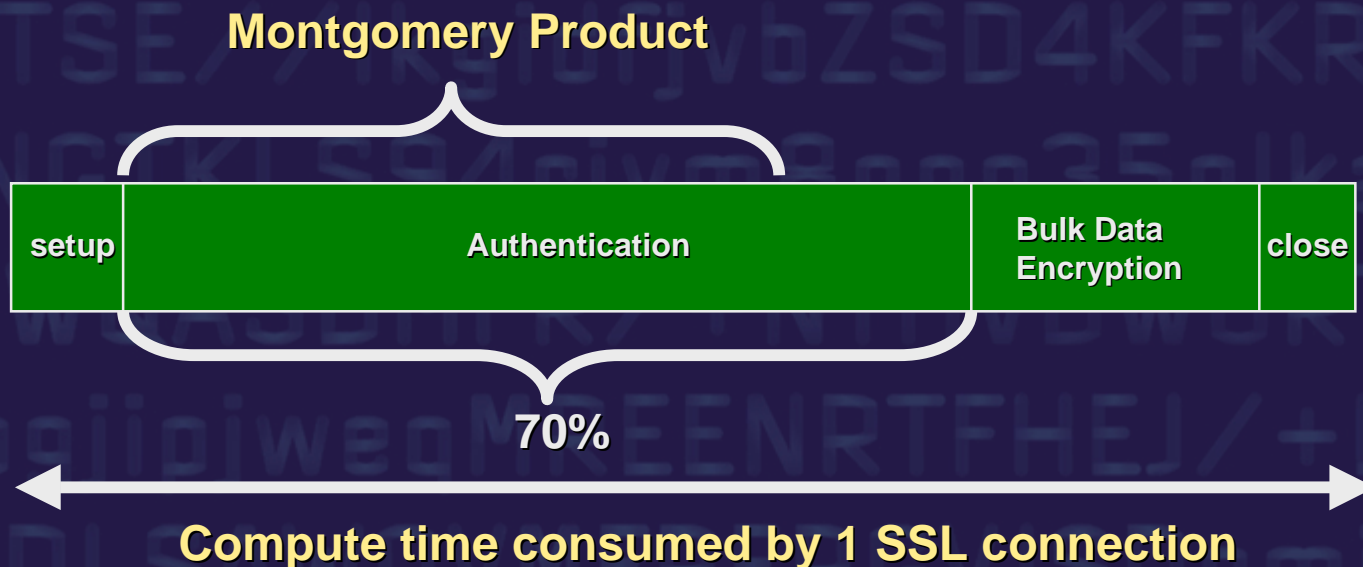
**Engines for e-Business Performance & Flexibility
for Enhanced Business Agility**



All dates specified are target dates provided for planning purposes only and are subject to change.

Optimizing performance for SSL workloads

- Goal: Provide enhanced performance to increase the number of transactions with improved response time
 - Identify server performance issues in SSL
 - Optimize for both IA-32 and IA-64 processors
- Significant finding
 - Montgomery Product significant workload in SSL authentication
 - Typically 50% of compute time per transaction



Itanium™ Processor Features for High Performance

- Six parallel functional units
- Large number of registers for complex computations
- Software pipelining for reduction of code complexity
- Fully pipelined integer multiply-add instructions enables multiple operations simultaneously

**High performance on security algorithms enables
more transactions for e-Business**

Leading Industry ISVs Support IA-64

SECURE
COMPUTING

RSA
SECURITY

Entrust
TECHNOLOGIES

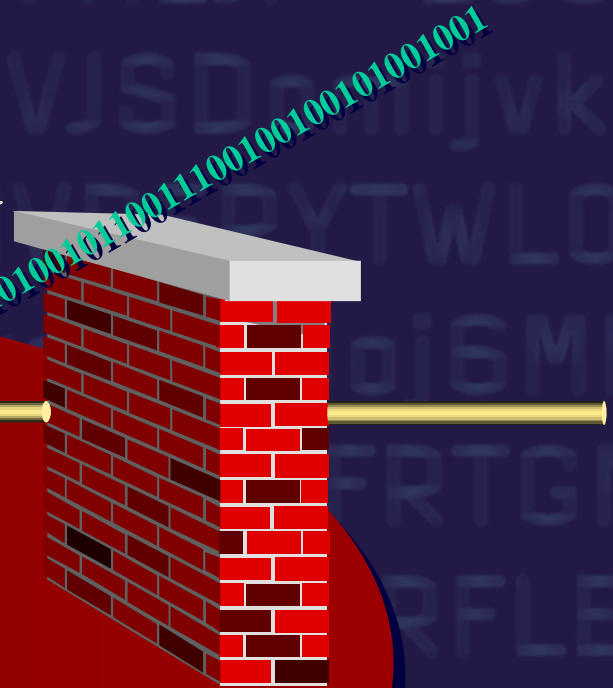
VeriSign


BALTIMORE
www.baltimoreinc.com

 **CHECK POINT**
Software Technologies Ltd.

Network Performance

Trusted Communications



Router/
Firewall



Server

Trusted Communications

IPSec - A Core Building Block of the Trusted Network

- **IPSec protected LAN communications with authentication and encryption**
- **Standards based - IETF standard (RFCs 2401-2411)**
- **Protects communication at network (IP) layer**
 - Transparent to applications
- **When to protect decided by “policy”**
- **Support a common set of standard algorithms**
 - Authentication - SHA-1 HMAC and MD-5 HMAC
 - Encryption - DES and Triple DES

IPSec is a key feature of Windows 2000*

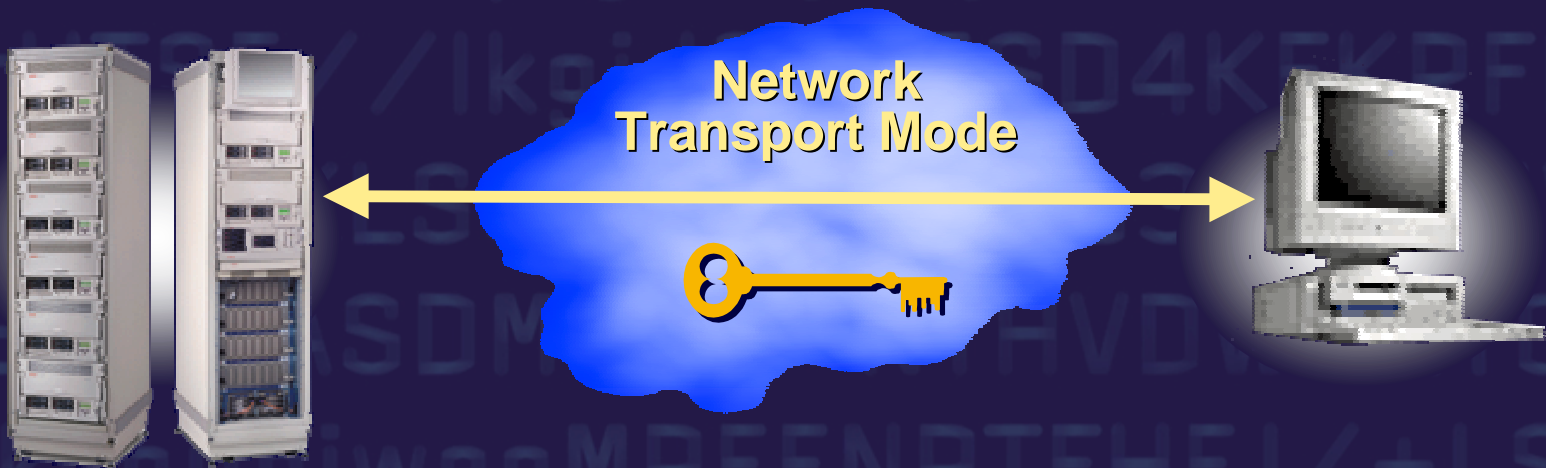


*Other brands and names are the property of their respective owners.

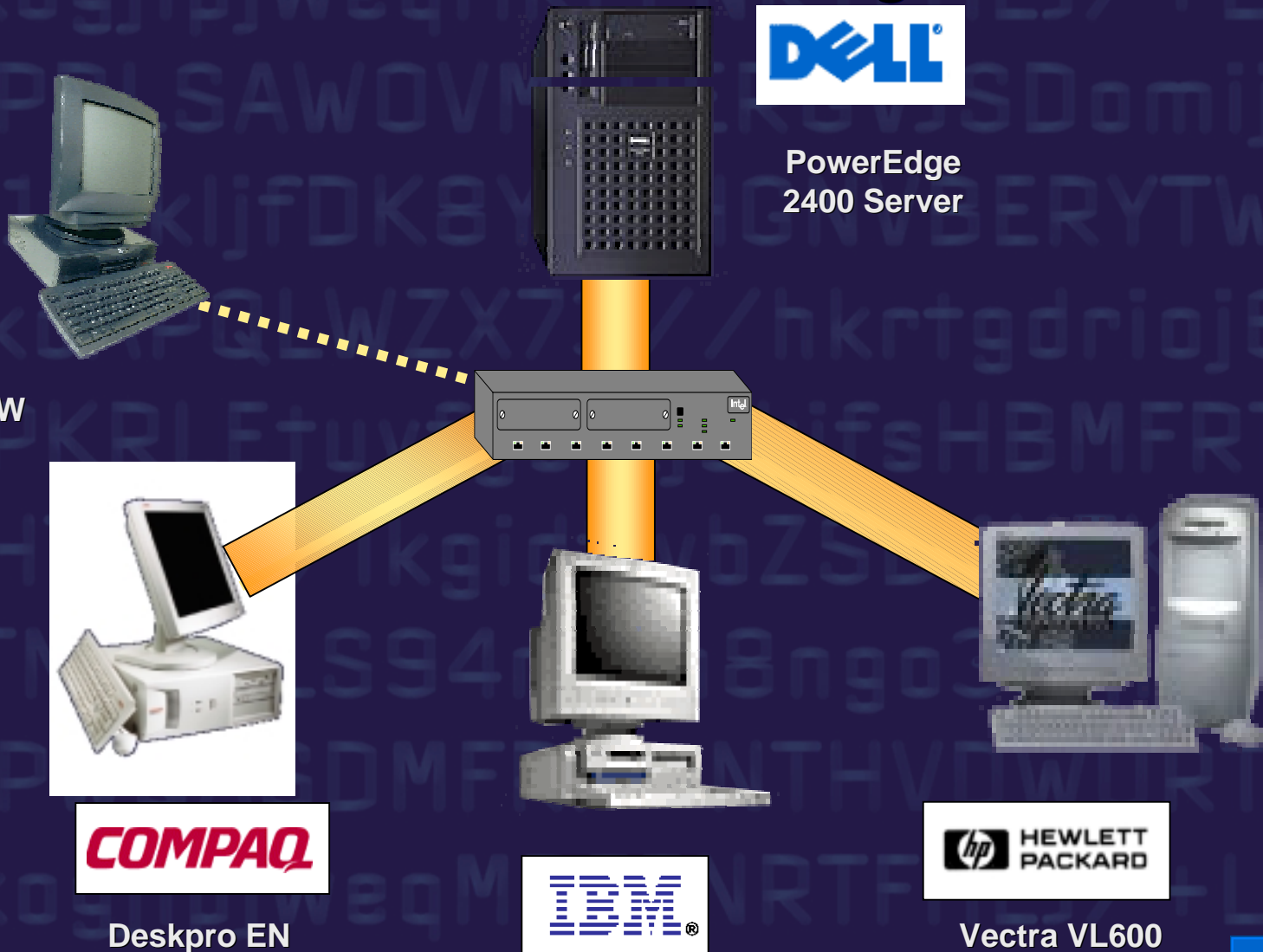
Trusted Communications

IPSec Transport Mode for the LAN

- Peer to peer communication
- Typically used in Intranet security
- Effective for protecting all workgroup communications



IPSec LAN Security



intel®

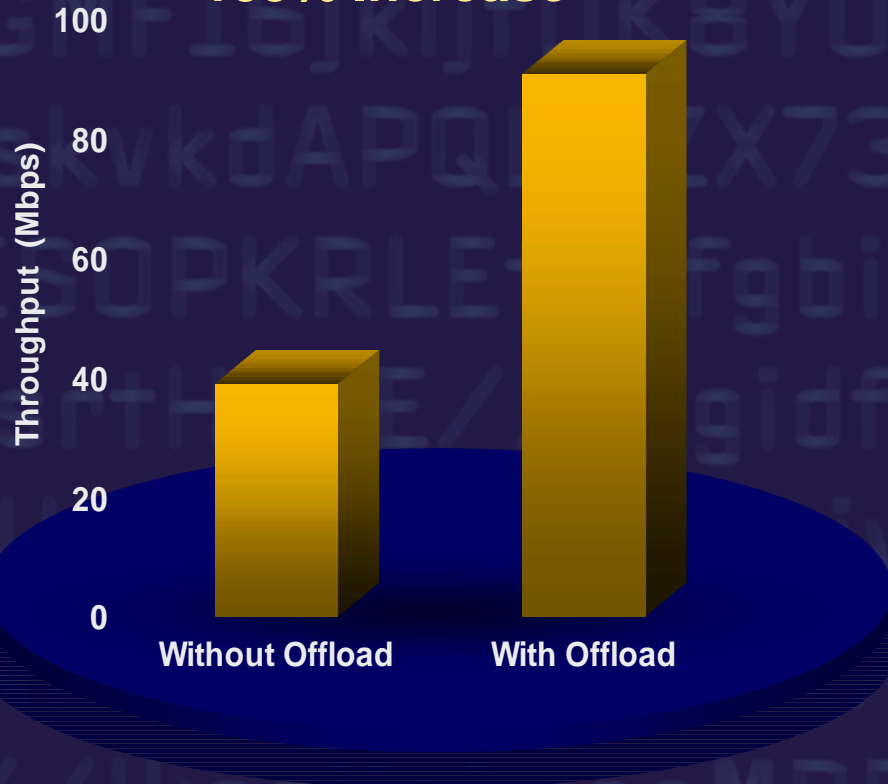
Other brands and names are the property of their respective owners.

Demo

IPSec Offload Performance

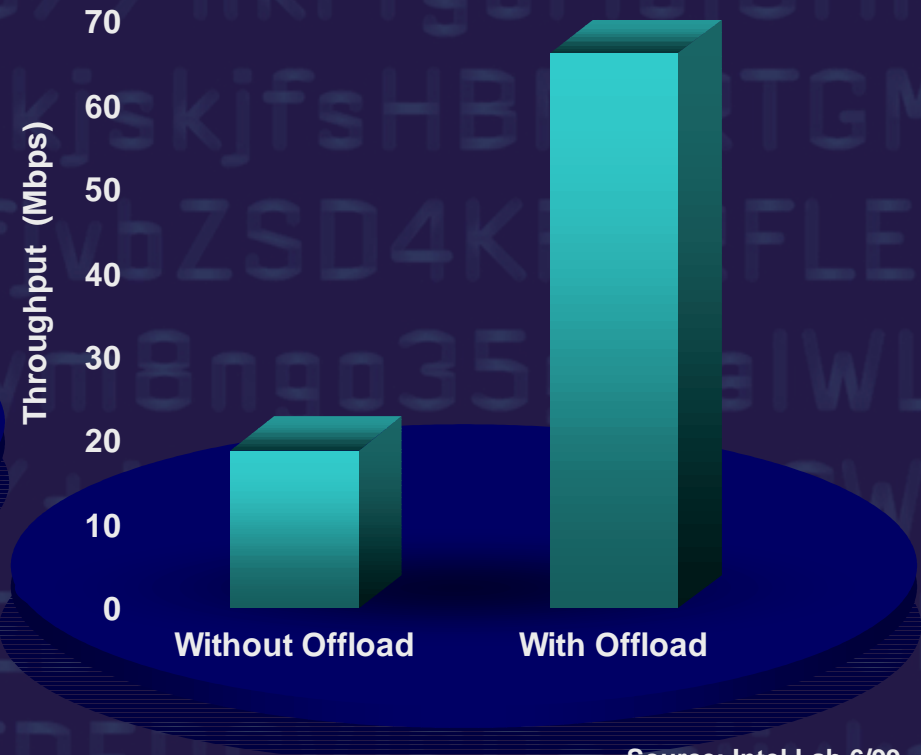
DES Performance

133% Increase



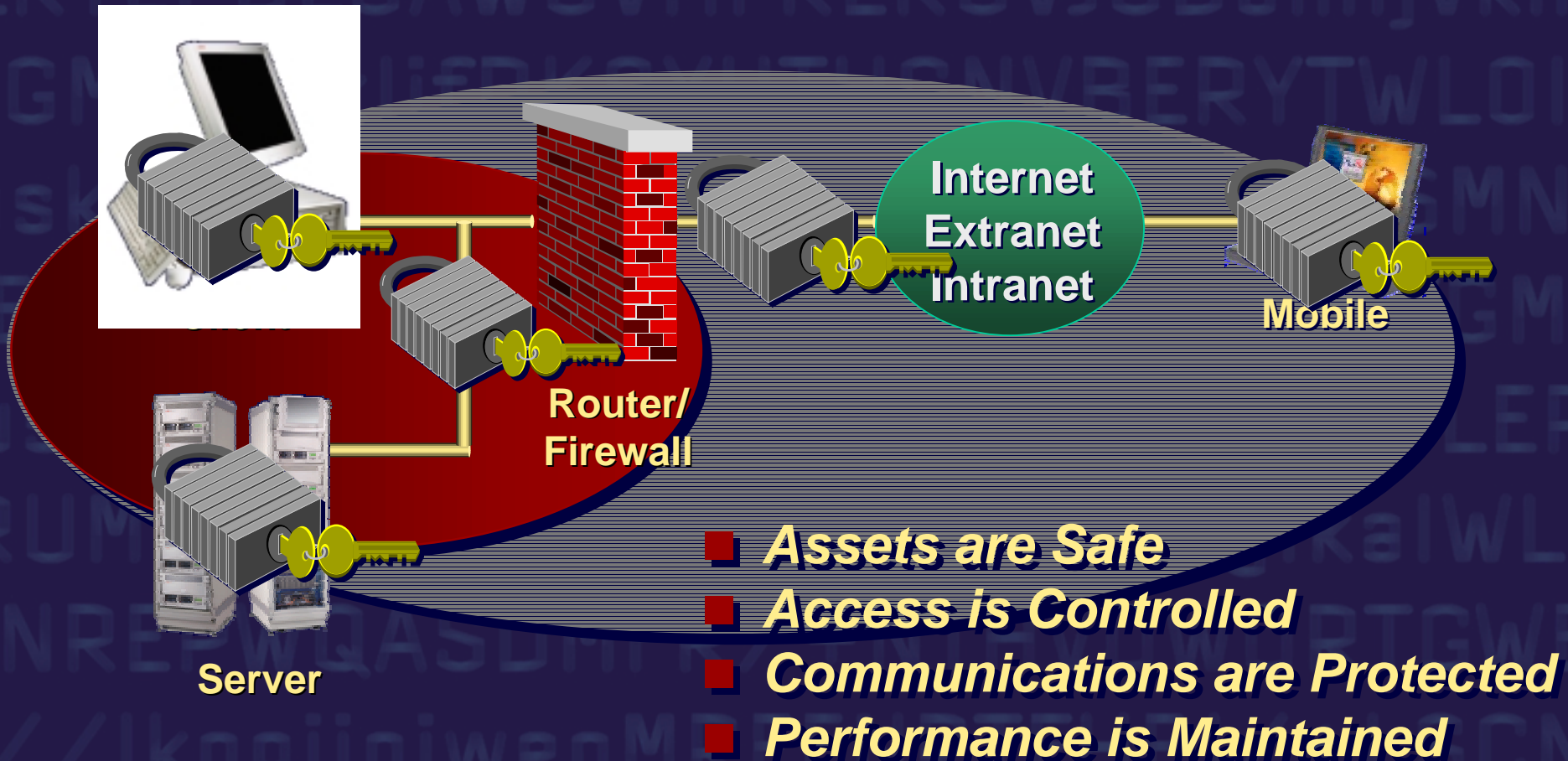
3DES Performance

250% Increase



The Trusted Enterprise

A Protected e-Business Environment



***It Takes an Industry to
Build a Trusted,
Connected World***



TCPA: Trusted Computing Platform Alliance

■ Mission

- **Develop new HW and SW specification (2H'00) for a truly trusted and protected PC platform based on common, open standards**
 - Ease the deployment, use and management of security elements on PCs
 - Complement new and existing security technologies
 - Ensure owner control of privacy
 - Encourage industry support and adoption

■ Steering Committee

- **Compaq, Hewlett Packard, IBM, Intel and Microsoft**
- **Working in conjunction with over 80 other industry participants**



<http://www.trustedpc.org>



PC/SC WG: PC Smart Card Workgroup

■ Mission

- Promote standards to ensure that smart card, smart card readers, and PCs interoperate
- Facilitate the development of smart card applications for computing platforms
 - Standardize SC and PC interfaces
 - Specify common control and programming interfaces
 - Help lower overall costs to facilitate widespread adoption
 - Encourage industry support and adoption

■ Core Members

- Bull, Gemplus, HP, IBM, Intel, Microsoft, Schlumberger, Siemens, Sun Microsystems, Toshiba



<http://www.pcscworkgroup.com>



CDSA Adopters

An open, cross-platform API for e-Business



THE *Open* GROUP

COMPAQ

intel.

IBM®

RAINBOW
TECHNOLOGIES
INTERNET SECURITY GROUP

hp HEWLETT
PACKARD

CYLINK



Worldwide
Information
Systems

CERTICOM

Lotus.

Bull

ValiCert

Chrysalis-ITS

AT&T

Information Security Corporation



MOTOROLA

intel®

CDSA V2 R 3.0 will ship in April 2000

Other brands and names are the property of their respective owners.

Working Together to...

- Establish standards and interoperability at each level of the HW & SW stack
- Enable “*One Virtual Network*”
- Deliver performance without compromise
- Promote common policies worldwide
- Intel is enabling security in Client, Server, Network and Service products

...Make it Mainstream!

intel®

<http://developer.intel.com/design/security/rsa2000>

intel®